UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ARBOR NETWORKS, INC., Plaintiff, v. WILLIAM E. RONCA III, RICHARD SHIRLEY, DOUGLAS FLEMING, JAMES GILL, JAMES NEEL, JASON MCEACHIN, MICHAEL L. PORTER, ANDREW HENKART, PAUL SCANLON, MICHAEL HOLLYMAN, and RED LAMBDA, INC., Defendants.	C.A. No. _______________

AFFIDAVIT OF CARLOS MORALES IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER AND MOTION FOR PRELIMINARY INJUNCTION

I, Carlos Morales, being duly sworn, do hereby depose and say as follows:

1. I am of legal age and believe in the obligation of an oath. I make the following Affidavit based on personal knowledge unless otherwise stated.

2. I am the Vice President - Sales Engineering and Operations for the Plaintiff in the above-captioned action, Arbor Networks, Inc. ("Arbor" or "Plaintiff").

3. I submit this Affidavit in support of Arbor's Motion for Temporary Restraining Order and Motion for Preliminary Injunction, filed contemporaneously herewith.

4. Arbor is a global provider of distributed denial of service ("DDoS") attack protection, network security, and visibility solutions. It performs detection and mitigation of security threats for both enterprise businesses (typically, large- and medium-sized enterprises such as banks) and carrier businesses (primarily, internet service providers ("ISPs").

5. Arbor has two main product lines, the Pravail product line (including the Pravail NSI and Pravail APS products), which is primarily sold to enterprise businesses, and Arbor Peakflow SP ("Peakflow"), which is primarily sold to carrier businesses.

6. Pravail NSI is a security intelligence solution that is used in an enterprise, government, or university network and allows the customer to monitor the actions of its network users as they relate to the network; for example, it provides customers with data regarding who is accessing the network, where they are accessing it, and when they are accessing it. Pravail NSI's purpose is to provide intelligence into threats such as malware, botnets, data theft and the inappropriate use of the network.

7. Pravail APS is used to both continuously monitor all traffic on the Internet border of enterprise or government datacenter networks, and provide pro-active protection against DDoS attacks on such networks. It is designed as a ready-to-use solution for DDoS protection with little operator intervention required.

8. Peakflow is a suite of solutions that are built for and marketed primarily towards ISPs, broadband providers, mobile providers, universities, datacenter operators and more complex enterprise networks. It provides extensive traffic visibility, statistical analysis of traffic on the network and DDoS protection. When a potential threat to the network is perceived and reported, Peakflow can redirect the threatening traffic to Arbor devices that "clean" and reroute healthy traffic back to the network, thereby defending against DDoS attacks and other threats. Peakflow also gives carrier businesses the ability to partition and deliver data, alerting, and mitigation specific to its own customers (for example, Peakflow allows an ISP to deliver to one of its customers, such as a bank, security services that specifically relate to network traffic to the bank's website).

9. The network security and anomaly detection industry is a highly competitive, specialized business and is becoming even more so with each passing year. Many markets and products within the industry are converging and blending together. Network security products that address different threats are increasingly becoming combined to create comprehensive solutions to customers' network security needs, eliminating the need for customers of these products to use multiple network security providers

[REST OF PAGE INTENTIONALLY LEFT BLANK]

The foregoing statements are made under the pains and penalties of perjury.

___/s/ *Carlos Morales*__________

Dated: July 19, 2012

Carlos Morales